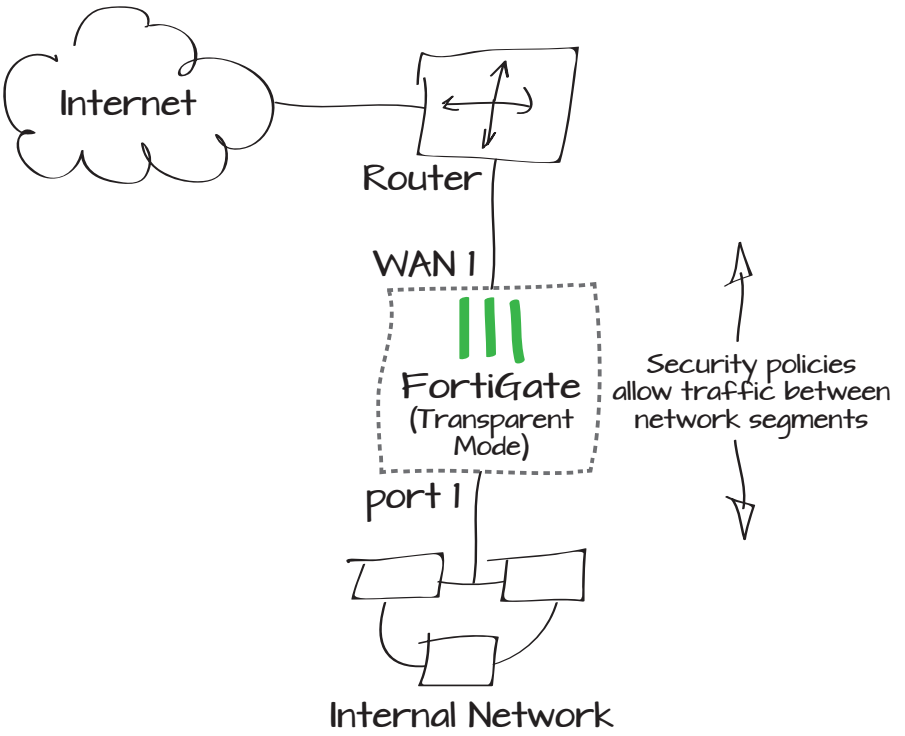
Adding a FortiGate unit without changing the network configuration

This section describes how to connect and configure a new FortiGate unit to protect a private network without changing the network configuration. This is known as Transparent mode and it allows you to add network security without replacing the router. The FortiGate unit blocks access from the Internet to the private network but allows users on the private network to connect to the Internet. The FortiGate unit monitors application usage and detects and eliminates viruses.

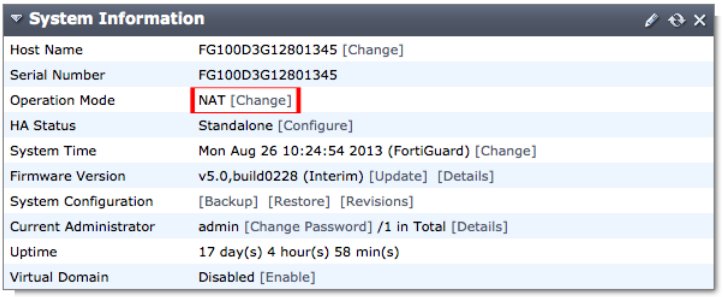
1. Connecting the FortiGate and configuring Transparent mode
2. Creating a security policy
3. Connecting the network
4. Results



Connecting the FortiGate and configuring Transparent mode

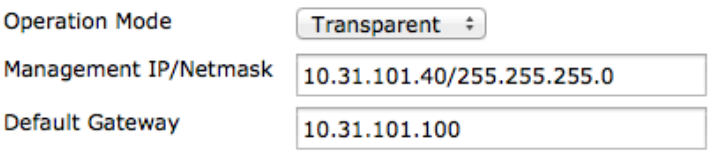
Changing to Transparent mode removes most configuration changes made in NAT/Route mode. To keep your current NAT/Mode configuration, backup the configuration using the System Information dashboard widget.

Go to **System > Dashboard > Status > System Information** and beside **Operation Mode** select **Change**.



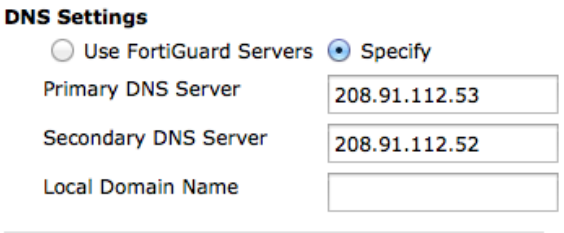
Set the **Operation Mode** to **Transparent**.

Set the **Management IP/Netmask** and **Default Gateway** to connect the FortiGate unit the internal network.



You can now access the web-based manager by browsing to the Management IP (in the example, you would browse to *https://10.31.101.40*).

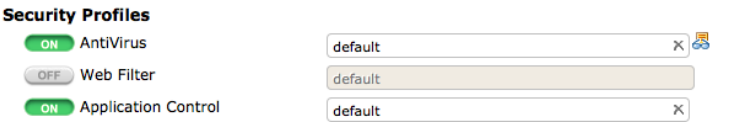
The FortiGate unit's **DNS Settings** are set to **Use FortiGuard Services** by default, which is sufficient for most networks. However, if you require the DNS servers to be changed, go to **System > Network > DNS** and add **Primary** and **Secondary** DNS servers.



Creating a security policy

Go to **Policy > Policy > Policy** and select **Create New** to add a security policy that allows users on the private network to access the Internet.

Under **Security Profiles**, enable **Antivirus** and enable **Application Control**.



Press **OK** to save the security policy

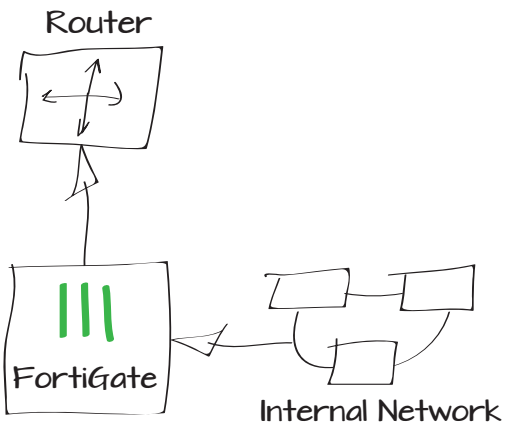
Power off the FortiGate unit.

Connecting the network

Connect the FortiGate unit between the internal network and the router.

Connect the wan1 interface to the router internal interface and connect the internal network to the FortiGate internal interface port.

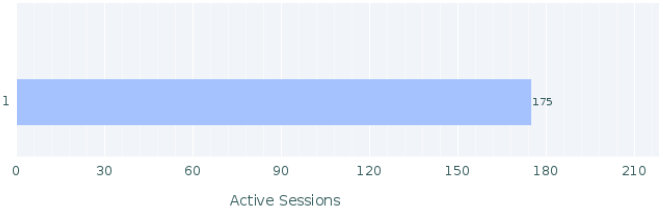
Power on the FortiGate unit.



Results

On the PC that you used to connect to the FortiGate internal interface, open a web browser and browse to any Internet website. You should also be able to connect to the Internet using FTP or any other protocol or connection method.

Go to **Policy > Monitor > Policy Monitor** to view information about the sessions being processed by the FortiGate unit.



Policy ID	Source Interface/Zone	Destination Interface/Zone	Action	Active Sessions	Bytes	Packets
1	port1	wan1	✔	175	6.29 MB	9,114

If a FortiGate unit operating in Transparent mode is installed between a DHCP server and PCs that get their address by DHCP, you must add a security policy to allow the DHCP server's response to get back through the FortiGate unit from the DHCP server to the DHCP client. The internal to wan1 policy allows the DHCP request to get from the client to the server, but the response from the server is a new session, not a typical response to the originating request, so the FortiGate unit will not accept this new session unless you add a wan1 to the internal policy with the service set to DHCP.